Security Patch Management
Preparing The Case for Automation

April 13, 2004

Overview

- Business Reasons for Implementing Automated Security Patch Management at FSA
- Current State of Vulnerabilities/Patch Release/Patch Application
- Highlights of Regulatory Requirements and Recommendations
- Methods of Security Patch Management
- Functional and Reporting Capability Primer on Automated Security Patch Management
- Recommended Strategy and Next Steps

Implementing Automated Security Patch Management at FSA is a Good Business Decision

1. To Manage Risk Relative To Patch Management

- Assess risk
- Determine acceptable level of risk (ALR)
- Mitigate risk
- Monitor system inventory

2. To Comply

- Validate Patch Levels and Compliance (IV&V)
- Mitigate Audit Findings
- Improved & More Efficient Reporting Capabilities to ED and FedCIRC

3. To Achieve Efficiencies, Consistency, Security, and Accountability

- Ease burden of system/network administrators
- Assure authenticity and integrity of patches
- Policy management with real-time reporting
- Transparency Into Contractor Operations

The State of Security Patch Management

- Patch Management has become widely recognized as a critical component to the information security program.
- Operating systems and applications have become more sophisticated and require more code.
- In commercial software, there are from 5 to 20 bugs in every 1000 lines of code. Commercial Unix consists of between 500,000 and 1 million lines of code.

The State of Security Patch Management

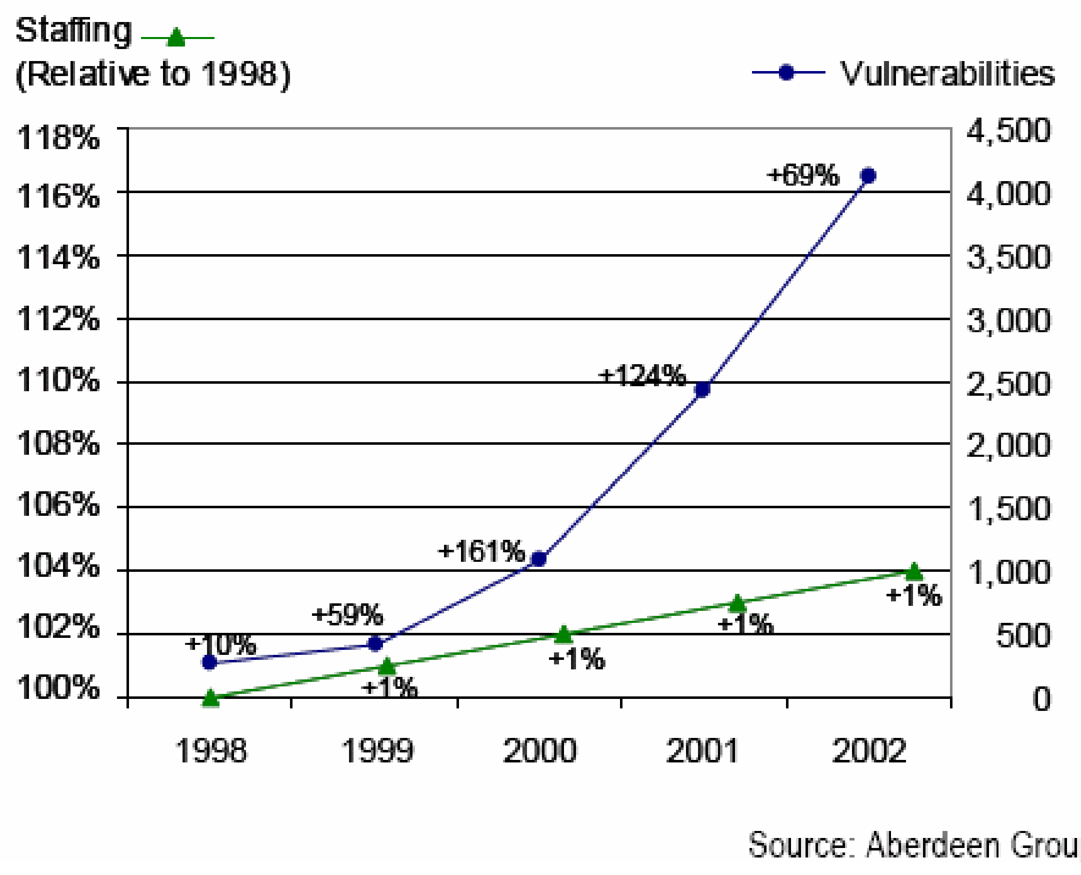
- Gartner reports that 90% of security exploits are carried out through vulnerabilities for which there are known patches

- The pace of discovery of security related bugs/vulnerabilities is attributable to exponential growth of connectivity, increase of skilled and unskilled incidents, and security vendor white hat activity.

- The gap between vulnerability and exploit is shrinking and has become shorter than the ability to patch in many cases.

The State of Security Patch Management

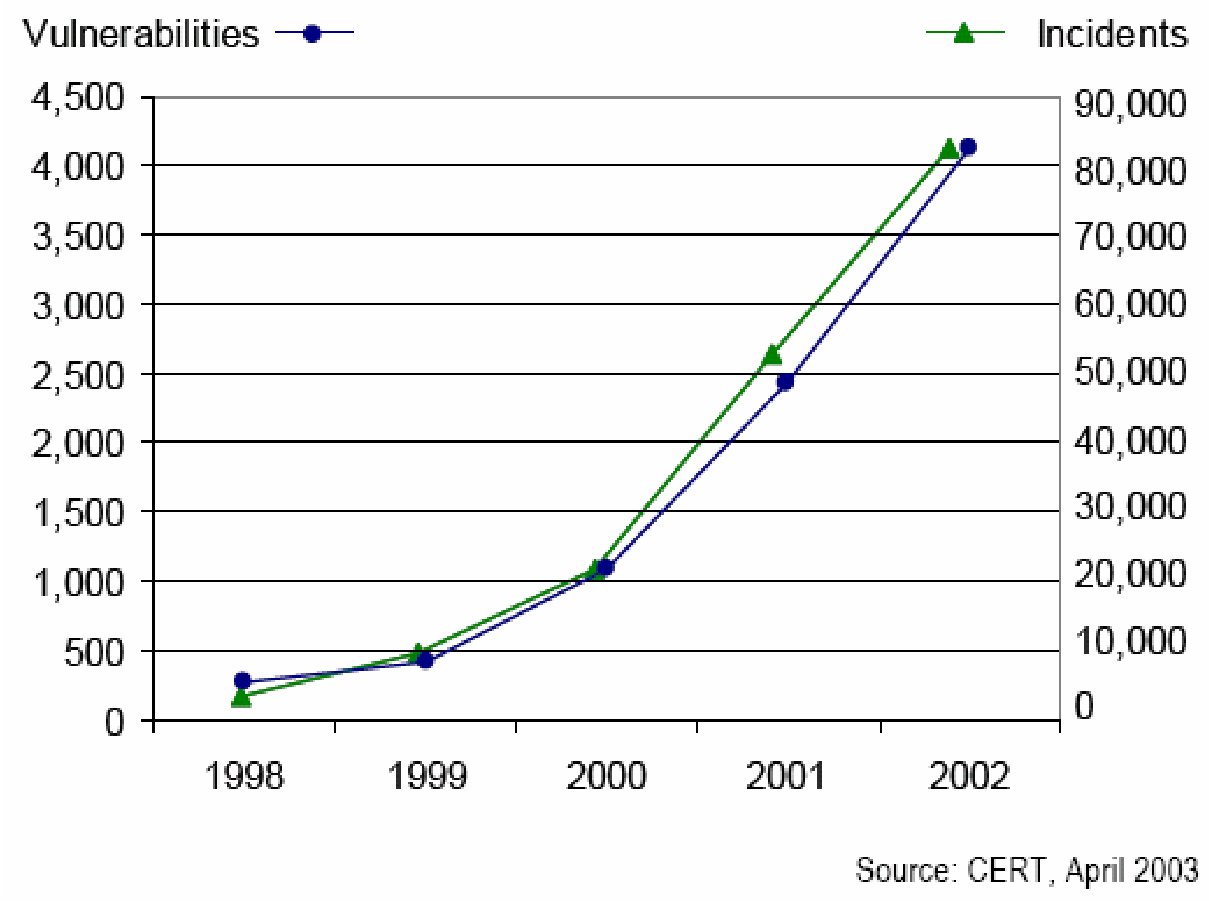
Vulnerability Growth v. Staffing Increases



Source: Aberdeen Group, May 2003

The State of Security Patch Management

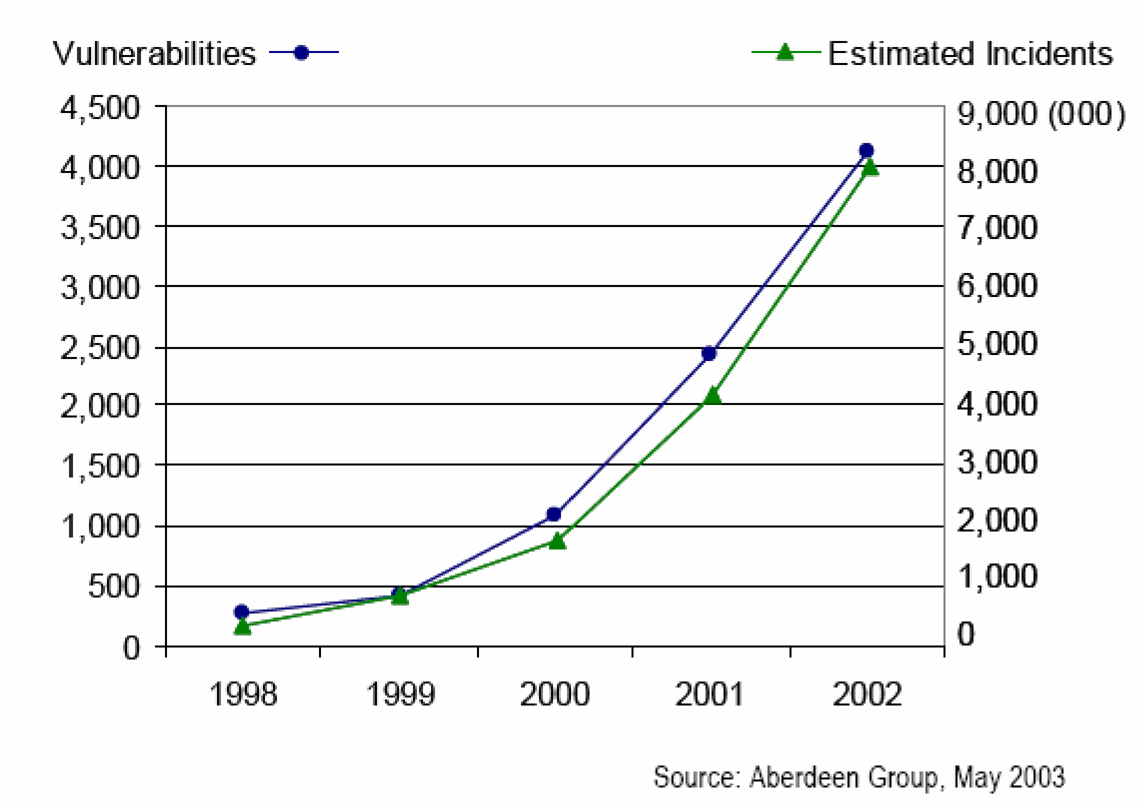
Reported Incidents keeping pace w/ vulnerabilities



Source: CERT, April 2003

The State of Security Patch Management

Estimated *Total* Incidents Are One Hundred Times Those Reported



Source: Aberdeen Group, May 2003

Legal & Regulatory Requirements/Recommendations

Requirements and recommendations for Security Patch Management Can Be Found In:

- Federal Information Security Management Act (FISMA) of 2002
- Appendix III to OMB Circular No. A-130 Security of Federal Automated Information Resources
- GAO House Testimony of Wednesday, September 10, 2003
- NIST 800-40 Procedures For Handling Security Patches
- NIST 800-61 Computer Security Incident Handling Guide
- NIST 800-26 Self Assessment Guide
- ED Security Policy Handbook
- FSA Information Technology Security and Privacy Policy
- ED System Security Plan Template

Legal & Regulatory Requirements/Recommendations (Cont.)

FISMA (section 3544(b)(2)(B) and (C) , (section 3544(b)(2)(D)(iii)) , (section 3544(b)(5)(A) and (B), & (section 3544(b) (6) and (7)(A))

- **In accordance with FISMA's Configuration Management and Lifecycle guidelines, given current conditions, and taking into account acceptable level of risk, *patch management* should utilize advanced methods of deployment, testing, monitoring and reporting.**

- **FISMA requires a patch management policy and that senior management acknowledge it as a critical component to the success of an agency's security program.**

- **Reactive, decentralized, manual or semi-automatic means of patch management are no longer viable.**

Sec. 3544. Federal agency responsibilities

(b) implement security program that includes--

(2) Policies and procedures that--

(B) cost-effectively reduce information security risks to an acceptable level;

(D) ensure compliance with–

(iii) minimally acceptable system configuration requirements, as determined by the agency

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing--

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c)

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including--

"(A) mitigating risks associated with such incidents before substantial damage is done;

Legal & Regulatory Requirements/Recommendations (Cont.)

August 6, 2003 Memorandum from Director of OMB

References FISMA (section 3544(b)(2)(D)(iii)) and comments as follows:

The necessary depth and breadth of an annual FISMA review depends on several factors such as: 1) the acceptable level of risk and magnitude of harm to the system or information; 2) the extent to which system configurations and settings are documented and continuously monitored; **3) the extent to which patch management is employed for the system;** 4) the relative comprehensiveness of the most recent past review; and 5) the vintage of the most recent in-depth testing and evaluation as part of system certification and final accreditation.

Legal & Regulatory Requirements/Recommendations (Cont.)

August 6, 2003 Memorandum from Director of OMB (Cont.)

For example, if in the previous year a system underwent a complete certification and received final (not interim) authority to operate, has documented configuration settings, employs automated scanning tools to monitor configurations, threats, and vulnerabilities,

and has an effective patch management capability, a simple maintenance review using NIST’s self assessment tool may meet the FISMA annual review requirement.

If none or only some of the foregoing are true, then the annual testing and evaluation must be far more comprehensive commensurate with the acceptable level of risk and magnitude of harm.

Legal & Regulatory Requirements/Recommendations (Cont.)

August 6, 2003 Memorandum from Director of OMB (Cont.)

FISMA (section 3544(b)(2)(D)(iii)) requires that each agency develop specific system configuration requirements that meet their own needs and ensure compliance with them.

This provision encompasses traditional system configuration management, employing clearly defined system security settings, and **maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.**

Legal & Regulatory Requirements/Recommendations (Cont.)

United States General Accounting Office (GAO)

Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform
Wednesday, September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

Statement of Robert F. Dacey, Director, Information Security Issues

- Patch management can be an important element in mitigating the risks associated with software vulnerabilities, part of overall network configuration management and information security programs

- The challenge will be ensuring that a patch management process **has adequate resources and appropriate policies, procedures,** and **tools to effectively identify vulnerabilities and patches** that place an entity's systems at risk**.** Also critical is the capability to **adequately test and deploy the patches**, and then **monitor progress** to ensure that they work.

- Entities may also need to develop better relationships with their vendors to be alerted to vulnerabilities and patches prior to public release. In addition, software vendors may provide automated tools with customized features to alert system administrators and users of the need to patch, and if desired, automatically apply patches

- Services and Tools Also Provide Means for Improving Patch Management

Legal & Regulatory Requirements/Recommendations (Cont.)

NIST 800-40 Procedures for Handling Security Patches

Executive Summary Recommendations:

- Having an **explicit and documented patching and vulnerability policy** and a systematic, accountable, and documented process for handling patches.
- Creating an organizational **hardware and software inventory**
- **Identifying newly discovered vulnerabilities and security patches**
- **Prioritizing patch application**
- Creating an organization-specific **patch database**
- **Testing patches** for functionality and security (to the degree that resources allow)
- **Distributing** patch and vulnerability information to local administrators
- **Verifying** patch installation through network and host vulnerability scanning
- **Training** system administrators in the use of vulnerability databases
- Deploying patches **automatically** (when applicable)
- Configure **Automatic** Update of Applications (when applicable).

Legal & Regulatory Requirements/Recommendations (Cont.)

NIST 800-61 Computer Incident Handling Guide

NIST
National Institute of Standards and Technology

3.12 Preventing Incidents

Patch Management. Many information security experts agree that a large percentage of incidents involve exploitation of a relatively small number of vulnerabilities in systems and applications. Large organizations should implement a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches.

4.4.1 Choosing a Containment Strategy

Correct the Vulnerability or Weakness That Is Being Exploited

If an unpatched operating system is susceptible to a DoS from specially crafted packets, patch the operating system.

Legal & Regulatory Requirements/Recommendations (Cont.)

NIST 800-26 Self-Assessment Guide

Appendix A - System Questionnaire
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?

14.2.1 Is incident information and common vulnerabilities or threats shared with system owners of **interconnected systems**?

Appendix C - Federal IT Security Framework Level 4
5.2.b **Mechanisms** for identifying vulnerabilities revealed by security incidents of security alerts - ...In addition they should review security alerts issued by FedCIRC, vendors, and others

5.2.c **Process for reporting significant security weaknesses and ensuring effective remedial action**. - Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and **follow-up reviews** to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.

Legal & Regulatory Requirements/Recommendations (Cont.)

ED Information Technology Security Policy Handbook

IT configuration management controls must include mandatory installation, verification and management of software patches and fixes on all Department servers, workstations and laptops within 30 days of release, or sooner, as security issues dictate.

Legal & Regulatory Requirements/Recommendations (Cont.)

FSA Information Technology Security Policy

3.7 Configuration Management

Every FSA System Manager must create a configuration management plan that describes the *hardware and software maintenance controls* in place and the process by which configuration controls will be maintained for that system.

3.7.2.1 Maintenance and Repair

FSA System Managers must implement access controls and *other security precautions to prevent potentially malicious code, such as "back doors"*, from being used to evade authentication and authorization protections

System Managers must periodically must review their systems for *known vulnerabilities and current installation of software patches*. These reviews are separate from the C&A review conducted by the DAA.

3.7.2.2 Unapproved Software

The department must perform periodic audits of FSA computers to make sure *users do not install unapproved software.*

3.8 Incident Response

The confidentiality, integrity, and availability of FSA networked systems will depend in part on the preventative security measures to deter or inhibit attacks.

3.8.1 Information Sharing

FSA must share information regarding incidents and common vulnerabilities or threats with FSA system personnel and appropriate managers of systems and networks interconnected with FSA and with the department level security office.

Methods of Security Patch Management

- **Manual & Ad Hoc or Manual & Policy Driven**
  - Administrator manually going from machine to machine; surveying the machine’s applications, checking the app vendor’s website for updates, downloading the updates, installing (and rebooting in many cases) one-by-one.
- **Auto-Detect/Auto-Install**
  - Configuring machine/applications to auto-detect for and auto-install available critical patches for OS/applications from vendors that offer the service.
- **Automated, Centralized, Vendor Specific Service(s)**
  - Most common is Microsoft SMS using scripts, free product SUS (software update service – soon to be called WUS or Windows Update Service)
  - Sometimes augmented w/ additional functionality by using scripts
- **Hybrid approach**
  - Network personnel manage the network environment including patches/updates/signatures to NOS, antivirus, firewalls, and IDS; print and communication servers and other attached appliances; centralized productivity applications and repositories
  - System Owners manage updates and patches in accordance w/ security policy, configuration mgmt., and change mgmt. Procedures
- **Automated, Centralized, Multi-Platform Security Patch Management System**

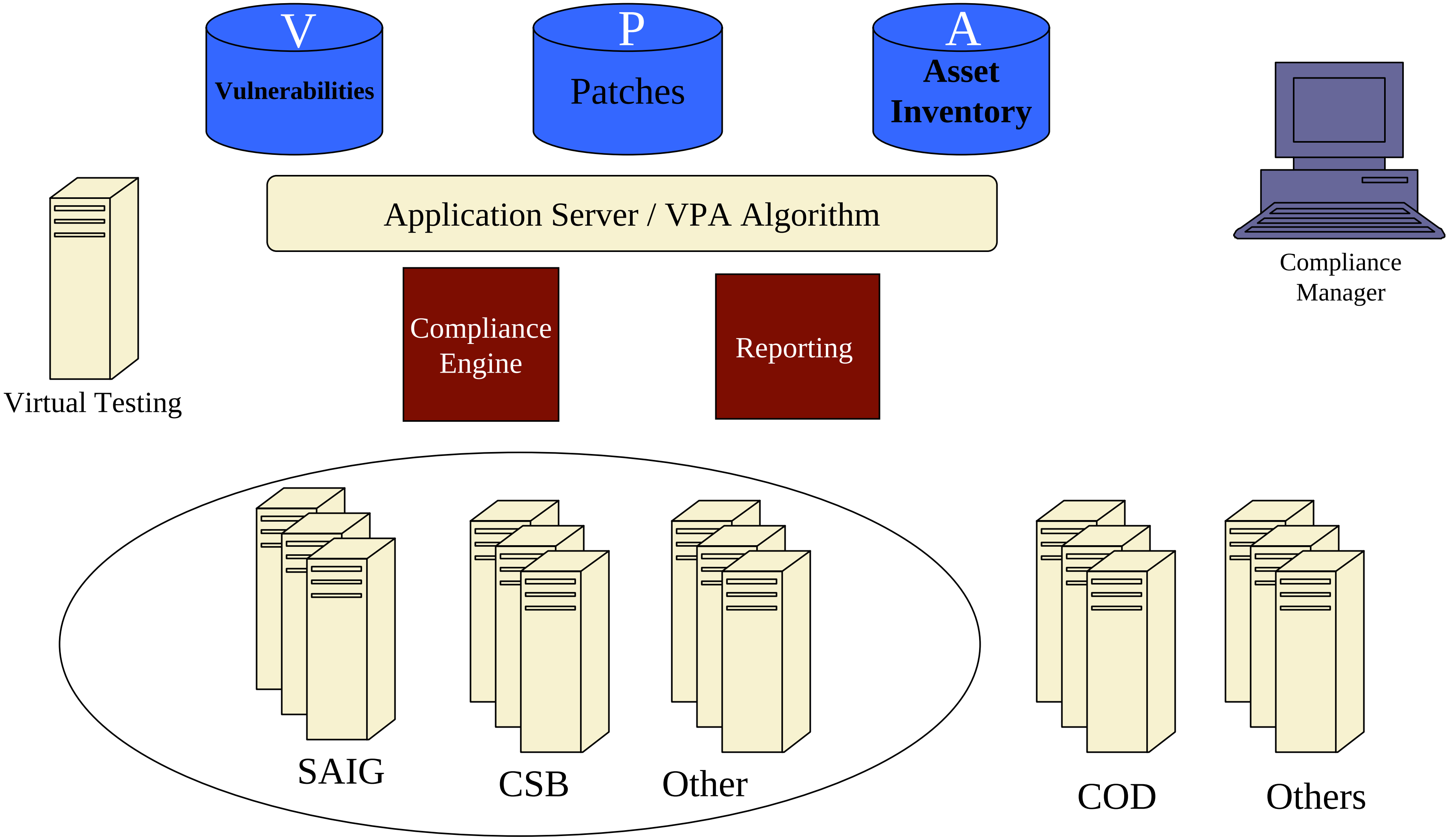
FSA's Automated Patch Management Solution Would…

I. Provide & Encourage Accountability	II. Ensure Consistency and Reliability	III. Introduce Added Security	IV. Create Efficiency
▪ Provide comprehensive reporting including remediation history, audit trails and trend analysis, and aggregated reports across multiple systems throughout the network ▪ Separate sets of computers and patch management administration and reporting capabilities into containers. Each group has properties that include members, client agent policy and mandatory patch baseline policy.	▪ Consistently monitor for changes ▪ Use patch signatures and master patch archive repository to scan system to **determine applicable patching and if prerequisites are met**. **Automatically calculate interdependencies** (customizable) ▪ **Give administrators control over updates/patches**	▪ Include disaster recovery features that enable automatic recovery from system failure such as hard disk crashes and server hardware failure. ▪ Provide rollback/uninstall capabilities to restore systems adversely impacted by patches.	▪ Central database of the latest patches, incidents, and methods for mitigating risks before a patch can be deployed or a patch has been released. Handle OS Windows NT/2000/2003, Windows 95/98/ME, Linux, Solaris, AIX, HP-UX, Mac, and Novell Netware, Oracle and ability to customize. ▪ Allow updates or packages to be downloaded in the background and/or auto-installed using secure identification and authentication to register against the server database.

FSA’s Automated Patch Management Solution Would… (Cont.)

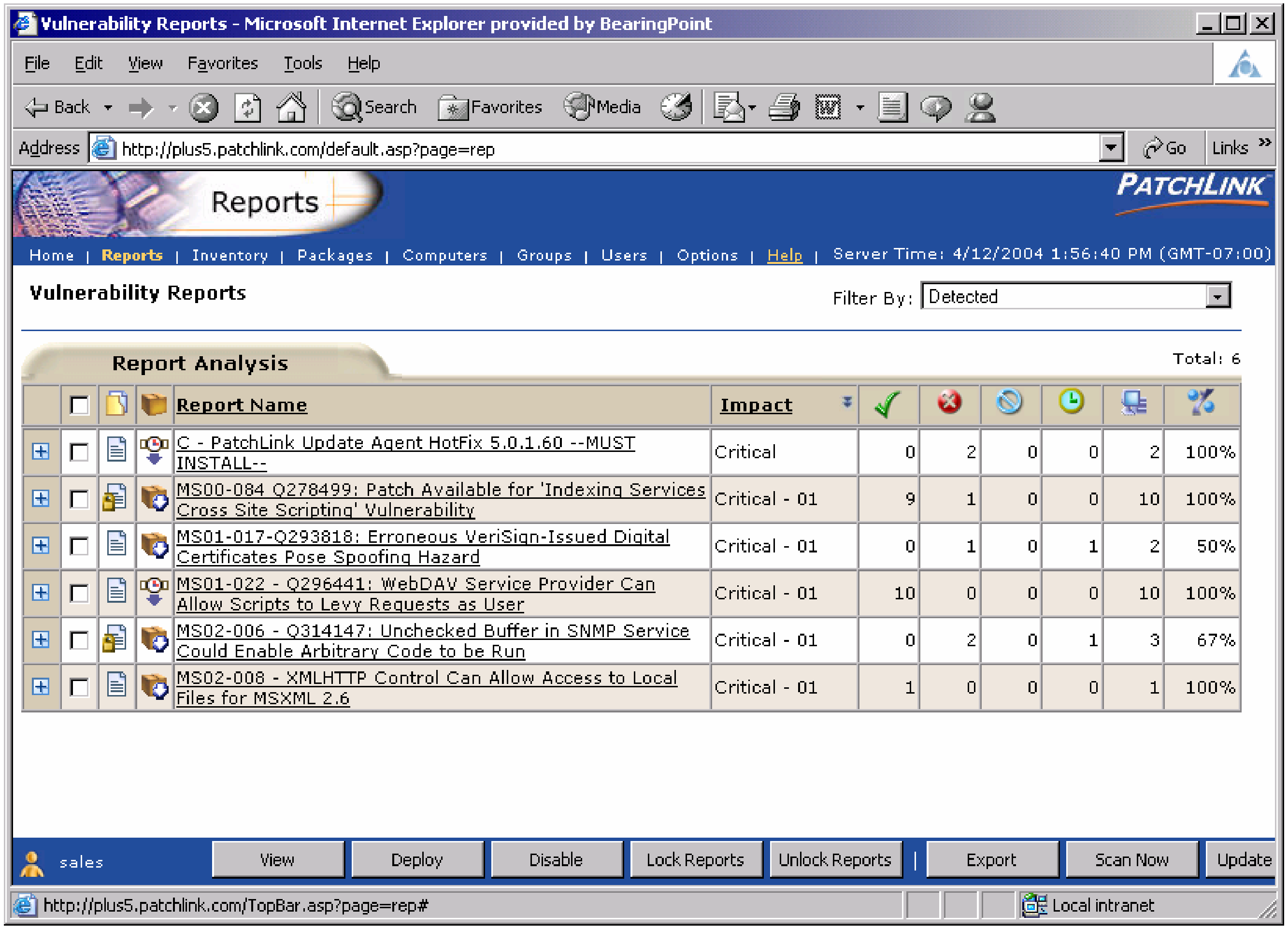
I. Provide & Encourage Accountability	II. Ensure Consistency and Reliability	III. Introduce Added Security	IV. Create Efficiency
▪Include canned and customizable graphical reporting including patch status for all computers, patch status for all vulnerability reports, status for all machines, compliance status for all groups. ▪Possess tools to enable customization of delivery, policy and reporting.	▪ Employ software inventory **change control**, service change control, and hardware change control ▪ Enforce security patch policy using **automatic deployment by group.**	▪Authentication and integrity protection of patches should be assured by using digital certificates, CRC checks, compression, and encryption on each file.	▪Enable multiple patch updates or patch chaining with a single reboot by creating executable to install DLLs, registry entries, etc. in order specified or applied before reboot. ▪ Support testing of patch with pre-testing against common configurations or supplied image ▪ Provide download resumption feature ▪ Do "network throttling" to control bandwidth use ▪ Provide status, new patch email notification ▪ Allow remote agent install and configuration ▪ Inventory computers and the software applications and patches installed

Automation Components



Reporting and Monitoring

Real-Time View of Vulnerability and Remediation State


Vulnerability Reports - Microsoft Internet Explorer provided by BearingPoint
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://plus5.patchlink.com/default.asp?page=rep
Go Links
Reports
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help | Server Time: 4/12/2004 1:56:40 PM (GMT-07:00)
sales
View Deploy Disable Lock Reports Unlock Reports | Export Scan Now Update
http://plus5.patchlink.com/TopBar.asp?page=rep#
Local intranet

Vulnerability Reports

Filter By: Detected

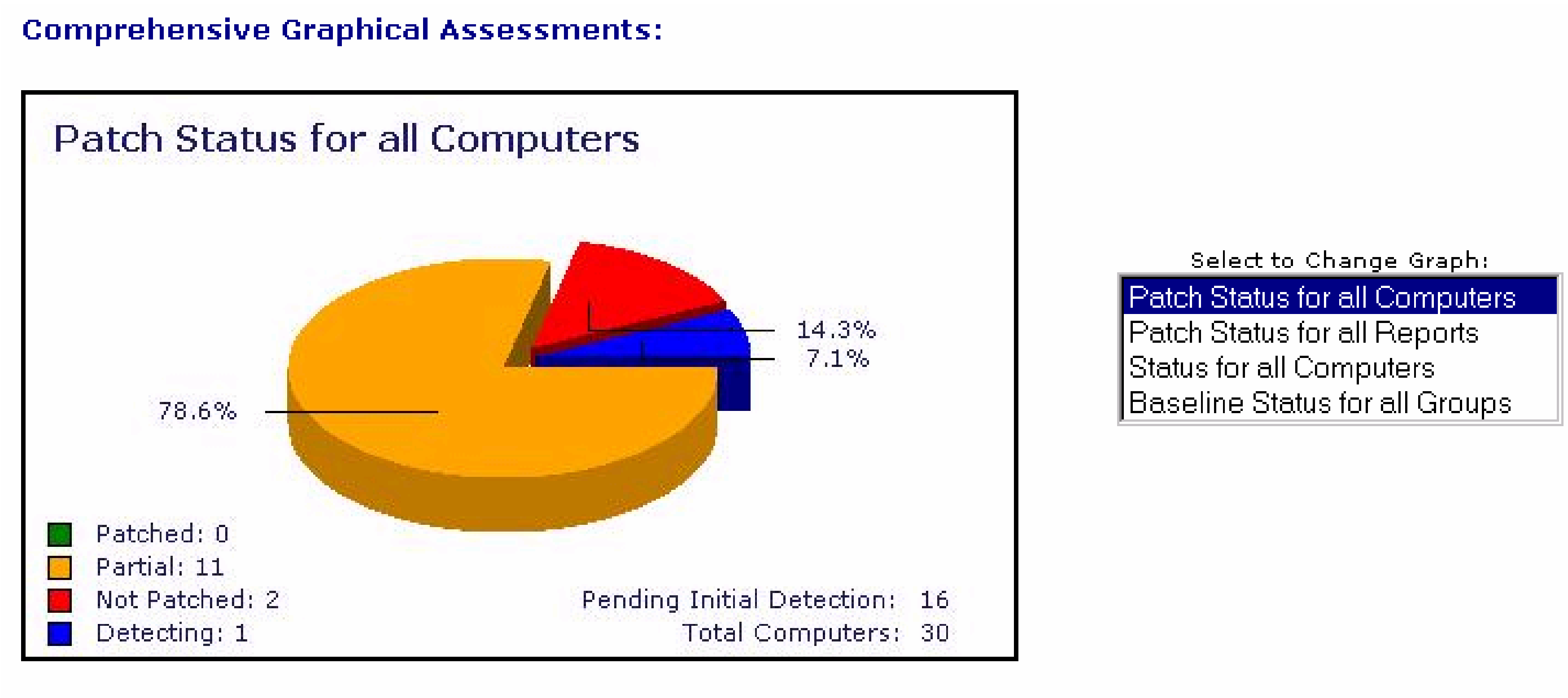
Report Analysis

Total: 6

	□	Report Name	Impact	✓	✗	⊘	🕐	🖥	%
⊞	□	C - PatchLink Update Agent HotFix 5.0.1.60 --MUST INSTALL--	Critical	0	2	0	0	2	100%
⊞	□	MS00-084 Q278499: Patch Available for 'Indexing Services Cross Site Scripting' Vulnerability	Critical - 01	9	1	0	0	10	100%
⊞	□	MS01-017-Q293818: Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard	Critical - 01	0	1	0	1	2	50%
⊞	□	MS01-022 - Q296441: WebDAV Service Provider Can Allow Scripts to Levy Requests as User	Critical - 01	10	0	0	0	10	100%
⊞	□	MS02-006 - Q314147: Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run	Critical - 01	0	2	0	1	3	67%
⊞	□	MS02-008 - XMLHTTP Control Can Allow Access to Local Files for MSXML 2.6	Critical - 01	1	0	0	0	1	100%

Reporting and Monitoring

Customizable Aggregate and Trend Reports



Comprehensive Graphical Assessments:

Patch Status for all Computers

- 🟩 Patched: 0
- 🟧 Partial: 11
- 🟥 Not Patched: 2
- 🟦 Detecting: 1

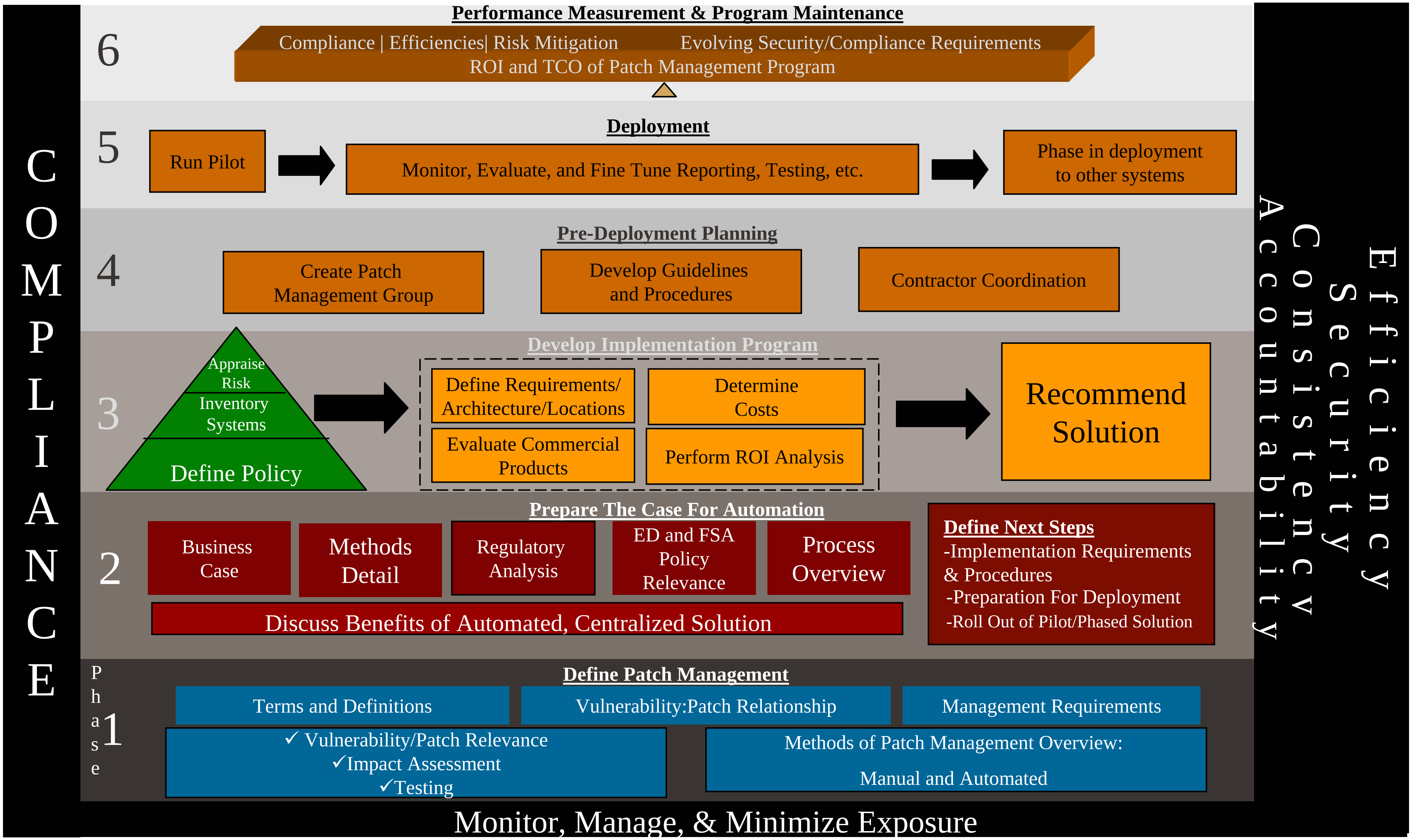
Pending Initial Detection: 16
Total Computers: 30

Select to Change Graph:
Patch Status for all Computers
Patch Status for all Reports
Status for all Computers
Baseline Status for all Groups

Recommended Strategy for Implementing Security Patch Management at FSA

1. Define patch management policy including what the policy is, why it is needed, the scope, and how and by whom it will be completed
2. Write and draft the policy
3. Inventory systems to include hardware, OS, applications, and means of connectivity
4. Examine the vulnerability:available patch:operational criticality state
5. Assess current patch management methods and testing procedures
6. Determine the actual risk
7. Devise plan for remediation
8. Implement automated solution
9. Measure Performance. Maintain Program.

Managing Software Vulnerability and Security Patch Management at FSA



COMPLIANCE

Efficiency

Security

Consistency

Accountability

6

Performance Measurement & Program Maintenance

Compliance | Efficiencies| Risk Mitigation

Evolving Security/Compliance Requirements

ROI and TCO of Patch Management Program

5

Deployment

Run Pilot

Monitor, Evaluate, and Fine Tune Reporting, Testing, etc.

Phase in deployment to other systems

4

Pre-Deployment Planning

Create Patch Management Group

Develop Guidelines and Procedures

Contractor Coordination

3

Develop Implementation Program

Appraise Risk

Inventory Systems

Define Policy

Define Requirements/ Architecture/Locations

Determine Costs

Evaluate Commercial Products

Perform ROI Analysis

Recommend Solution

2

Prepare The Case For Automation

Business Case

Methods Detail

Regulatory Analysis

ED and FSA Policy Relevance

Process Overview

Discuss Benefits of Automated, Centralized Solution

Define Next Steps

-Implementation Requirements & Procedures

-Preparation For Deployment

-Roll Out of Pilot/Phased Solution

Phase 1

Define Patch Management

Terms and Definitions

Vulnerability:Patch Relationship

Management Requirements

✓ Vulnerability/Patch Relevance

✓Impact Assessment

✓Testing

Methods of Patch Management Overview:

Manual and Automated

Monitor, Manage, & Minimize Exposure

🟦 Complete 🟥 In Draft/Review 🟧 Next Steps 🟩 Under Current Development 🟫 Waiting ⬛ Objectives